017.41038X00
NC 25879

SYSTEM AND METHOD OF PROVIDING VIRUS PROTECTION AT A GATEWAY

BACKGROUND OF THE INVENTION

Field of the Invention

[0001] The present invention relates to systems and methods for detecting the presence of computer viruses in data transmissions to networks, and a computer program which when executed detects viruses in the data transmissions to the networks.

Description of the Prior Art

[0002] The Assignee of the present invention sells a Web Shield™ product for Nokia Appliance V.2 which is a dedicated system optimized with antivirus capability. McAfee® antiviral software is utilized therein to provide complementary protection to existing desktop solutions. The Web Shield™ stops viruses within data packets at a gateway to a network before penetrating the network. As a result, the deficiencies of prior art desktop and server-based antiviral systems, which degrade performance of multipurpose systems, is avoided with the attendant potential for the multipurpose systems being compromised being eliminated. The Web Shield™ provides an additional layer of protection to existing antiviral software resident on PCs or other computers including servers.

[0003] The Web Shield stops viruses and malicious code threats, updates the scanning engine automatically with the latest virus definition file, scans inbound and outbound traffic, cleans, rejects or quarantines infected attachments, and has a simple configuration and management.

[0004] United States Patents 5,414,833, 5,623,600 and 6,275,942 disclose additional antivirus systems.

SUMMARY OF THE INVENTION

[0005] The present invention is a virus protection system, a method of providing virus protection which has an improved performance relative to the Web Shield™, and computer program stored on a storage medium for use in a virus scanning engine. The invention permits an early classification of the data packets so that it is possible to also route real-time traffic through a gateway which processes the data packets prior to testing with the virus scanning engine. The early classification improves the performance of the gateway. Furthermore, packets from the virus containing packet stream (or from the originating host) may easily be discarded by use of simple and fast firewall rules that are added when a virus is encountered. If viruses are found, the virus sending processor may be black listed so that no traffic from the virus sending processor passes the firewall in the future.

[0006] As used herein, the term "virus" includes any form of malicious executable code or malicious data threat including, but not limited to, "viruses" and "worms".

[0007] In accordance with the present invention, data packets are received by a firewall within a gateway at which they are tested and forwarded to a virus scanning engine. The virus scanning engine determines if the received data packets contain a virus. If so, the tested data packets are discarded and if not the tested data packets are forwarded to their destination to which the transmission of the data packets was made by a first network. Additionally, the firewall processes the received data packets in accordance with a packet classification criteria provided from a virus detection database to determine the presence of any data packets which cannot contain viruses, such as, but not limited to, audio and video stream data which are immediately forwarded to the destination so as to maintain real time data timing which is critical to data such as, but not limited to, audio and video streams. The virus scanning engine generates an alert which is transmitted to the firewall and the destination. The alert is utilized by the firewall to drop any data packets which are received in a data stream which has been determined to contain a virus. Additionally, the firewall may discard any other packets which are illegal for reasons other than the presence of a virus. A buffer storage is associated with the virus scanning engine which permits the data stream of packets to be sufficiently buffered in order to complete the necessary processing to determine the presence of a virus. Additionally, the virus scanning engine informs the destination of the data packets when the data packets are determined to contain a virus so as to prevent the destination from being infected with the virus. The virus scanning engine is coupled to a virus detection database which provides the necessary programming which is executed by at least one processor of the virus scanning engine for determining the presence of viruses in the data packets. Virus updates are provided to both the packet classification database and virus detection database so as to update the classification of the criteria used by the firewall to determine a first type of data packets which are immediately transmitted by the firewall to the destination for the reason that they are determined to not contain a virus and the second type of data packets which are forwarded from the firewall and received by the virus scanning engine at which they are tested to determine if they contain a virus. The virus detection database provides the latest antivirus detection programming to the at least one processor of virus scanning engine and may use any known type of anti-virus programming.

[0008] In a communication system including at least a first network coupled to a destination to which transmissions of the data packets are made from the first network to the destination, a system for providing virus protection in accordance with the invention includes a gateway coupled between the first network and the destination, which includes a firewall which receives the data packets and virus scanning engine, coupled to the firewall, which receives the data packets after reception by the firewall, tests the data packets, passes any data packets, which are tested to not contain a virus to the destination and discards any data packets which are tested o contain a virus. The firewall may classify the received data packets into packets of a first type which cannot contain a virus and second type which can contain a virus and may forward the data packets of the first type to the destination without testing by the virus scanning engine and may forward the data packets of the second type to the virus scanning engine for testing thereof. The virus scanning engine may test the data packets of the second type and may forward those data packets of the second type which are tested to not contain a virus to the destination. The data packets of the first type may contain real time data. The virus scanning engine may, when a virus is detected, alert the firewall that a virus has been detected which, in response to the alert, may stop reception of a data stream containing the data packets. A buffer may store the data packets of the second type while the virus scanning engine is processing the data packets of the second type to detect a virus. The firewall may drop any received data packets which are tested to be illegal according to firewall rules. A packet classification database, coupled to the firewall, may provide information to the firewall which defines the first and second types of data packets; and a virus detection database, coupled to the virus scanning engine, may provide programming controlling the testing of the data packets of the second type by the virus scanning engine. The virus scanning engine, upon detection of a virus in the data packets, may also alert the destination that a virus has been detected. The destination may be a local area network, a personal computer, or a second network. The first network may be a wide area network which may be the Internet. The first network may be the Internet; and the destination may comprise an Internet service provider coupled to the gateway, a modem coupled to the Internet service provider and one of a local area or personal computer coupled to the modem. The virus scanning engine may decode the data packets during determination if the data packets contain a virus. The virus scanning engine may function as a proxy for a destination processor which receives the data packets.

[0009] In a communication system including at least a first network coupled to a destination to which transmissions of data packets are made from the first network to the destination, a gateway coupled between the first network and the destination which includes a firewall which receives the data packets and a virus scanning engine, a method in accordance with the invention includes receiving the data packets at the firewall; transmitting the received data packets from the firewall to the virus scanning engine; testing the data packets with the virus scanning engine; and transmitting from the virus scanning engine any data packets which are tested by the virus scanning engine to not contain any virus to the destination and the discarding any data packets which are tested to contain a virus.

[0010] A computer program stored on a storage medium for use in a virus scanning engine in a communication system including at least a first network coupled to a destination to which transmissions of data packets are made from the first network to the destination, a gateway coupled between the first network and the destination, which includes a firewall which receives the data packets and the virus scanning engine, coupled to the firewall, which receives the data packets after reception by the firewall, passes any data packets, which are tested to not contain a virus to the destination and discards any data packets which are tested to contain a virus, in accordance with the invention when executed causes the virus scanning engine to execute at least one step of testing the data packets for the presence of a virus. The firewall may classify the received data packets into packets of a first type which cannot contain a virus and second type which can contain a virus and may forward the data packets of the first type to the destination without testing by the virus scanning engine and may forward the data packets of the second type to the virus scanning engine for testing thereof and wherein the computer program when executed causes the virus scanning engine to test the data packets of the second type and causes the virus scanning engine to forward those data packets which are tested to not contain a virus to the destination. The computer program when executed may cause the virus scanning engine to forward any data packets, which are tested to not contain a virus to the destination and may cause the virus scanning engine to discard any data packets which contain a virus. The data packets of the first type may contain real time data. The computer program, when executed, may cause the virus scanning engine, when a virus is detected, to alert the firewall that a virus has been detected which, in response to the alert, stops reception of a data stream containing the data packets. The firewall may drop any received data packets which are tested to be illegal according to firewall rules, a packet classification database may be coupled to the firewall which provides information to the firewall which defines the first and second types of data packets and a virus detection database may be coupled to the virus scanning engine and wherein the computer program controlling the testing of the data packets of the second type by the virus scanning engine may be provided by the virus detection database.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] Fig. 1 illustrates a block diagram of an exemplary system in which the present invention may be practiced.

[0012] Fig. 2 illustrates a block diagram of a first network in which the present invention may be practiced.

[0013] Fig. 3 illustrates a block diagram of a second network in which the present invention may be practiced.

[0014] Fig. 4 illustrates a block diagram of a third network in which the present invention may be practiced.

[0015] Fig. 5 illustrates a block diagram of a fourth network in which the present invention may be practiced therein.

[0016] Like reference numerals identify like parts throughout the drawings.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0017] Fig. 1 illustrates a block diagram of a system 10 in which the present invention is practiced. A first network 11, which may be of any known design, provides data packets including, but not limited to, data packets transmitted by the TCP/IP protocol to a gateway 12 which includes a firewall 14 which may be of any known design that receives the data packets. The data packets received by the firewall 14 are processed in accordance with a packet classification criteria which is stored in a packet classification database 16. The data packets are classified by the firewall 12 into a first type of data packets which cannot contain a virus in accordance with criteria specified by the packet classification database 16 and typically without limitation represent real time data. Those data packets of the first type which are determined as not possibly containing a virus are transmitted from the firewall 14 to their destination 18 including, but not limited to, the destinations set forth in the network architectures of Figs. 2-5 as described below. Without limitation, data packets of the first type, which are screened in accordance with the packet classification criteria provided by the packet classification database 16, are audio and video data streams. The output 20 is representative of n multiple ports from the firewall 14 with the payload of the data being provided on one or more output ports and further, additional information, not constituting the payload, which is used for setting up of the data transmission session being outputted on other ports 20. The firewall 14 forwards those data packets of the second type which may contain viruses to a virus scanning engine 22 of any known design at which at least one processor therein executes a computer program stored on any known type of storage medium as described below.

[0018] The processing of the data packets by the firewall 14 to divide them into first and second types provides an early classification of the packets so that real-time data traffic may be routed through the gateway to eliminate transmission of data packets to the virus scanning engine 22 which can reliably be determined to not contain viruses and which would slow down testing by the gateway 12 for viruses if forwarded to the virus scanning engine. Early classification improves the performance of the gateway 12 and further permits data packets from the virus containing packet stream (or from the originating host) to be readily discarded by use of simple and fast firewall rules that are added when a virus is encountered. If viruses are found, the virus sending processor may be black listed so that no traffic from the virus sending processor passes the firewall in the future.

[0019] The virus scanning engine 22 contains at least one processor which executes a program stored on a storage medium of any known type. The execution of the computer program causes processing of the data packets transmitted from the firewall 14 to the virus scanning engine 22 with virus detection criteria specified by virus detection database 24. The program may in addition control all facets of the operation of the virus scanning engine 22, as discussed below, including the reception of data packets of the second type from the firewall 14, the testing thereof, and the outputting of virus free packets and a virus alert to the firewall 14 and the destination 18 and control of communications between the virus detection database 24 and packet temporary storage 26. The virus detection database 24 is dynamically updated with virus updates which also update the packet classification database 16 to permit the criteria for screening the data packets into the first and second types to be dynamically varied to respond to changing or new viruses and data defining the first type or second types such as new types of data, which may be screened to determine that they do not contain viruses. The virus scanning engine 22 outputs the tested virus free data packets to the destination 18. A packet temporary storage 26 is associated with the virus scanning engine 22 to provide a buffer to permit storage of a sufficient number of data packets within a data stream being tested so as to permit determination if a data stream of data packets of the second type may be correctly determined to be virus free. If the virus scanning engine 22 detects the presence of a virus within the second type of data packets, an alert 28 is generated which is transmitted back to the firewall 14 and further to the destination 18. The alert 28, when transmitted to the firewall 14, provides a basis for instructing the firewall to drop data packets being received in the data stream which are determined to contain a virus. Additionally, the firewall 14 may drop data packets for other reasons in accordance with firewall rules. The main benefit of the firewall is to control and prevent outsiders from accessing the protected network (usually a LAN) behind the firewall. The data security inside the LAN does not have to be state-of-the-art if the firewall that connects the LAN, to the Internet or other wide area network, is robust. The firewall typically prevents data connections to be opened from the Internet or other wide area network and protects the machines in the LAN from different types of attacks (e.g. port scanning, Denial-of-Service attacks, etc.). The packet classification database 16 contains protocols, ports, packet lengths and other packet characteristics which are used collectively by the firewall 14 to perform the screening of the data packets so as to correctly identify those data packets of the first type which may be passed to the destination 18 on a real time basis and the data packets of the second type which are transmitted to the virus scanning engine 22 for testing for the presence of viruses. Additional information beyond that stored in the packet classification data base 16 may be used by the firewall 14 in determining if the received data packets are of the first type. As a result, real time video and audio streams and any other real time data which cannot contain viruses are not delayed by the virus scanning engine 22 so as to provide optimized performance. Moreover, eliminating data streams which contain data packets which are determined correctly as not being capable of containing viruses lessens the overhead on the testing process performed by the at least one processor executing the programming within virus scanning engine 22.

[0020] As a result of the splitting of the data packets into first and second types, which are respectively directly forwarded to the destination 18 and to the virus scanning engine 22, enhanced efficiency is obtained while permitting correct identification of data packets which contain viruses. Moreover, the packet temporary storage 26 has substantial capacity so as to permit a total data stream to be buffered when required for correct identification of a virus. But, in most applications, it is necessary only to test a much smaller number of data packets in while using the packet temporary storage 26 to determine whether the second type of data packets contain any viruses.

[0021] When the packet temporary storage 26 stores a total data stream, the virus scanning engine 22 acts as a proxy for the destination and may decode the data stream before forwarding to the destination 18. This may involve splitting of a TCP session or temporarily redirecting it to another location.

[0022] Fig. 2 illustrates a first network 100 in which the present invention may be practiced. The gateway 12 is coupled between the Internet 102 and a local area network 104.

[0023] Fig. 3 illustrates a second network 200 in which the present invention may be practiced. The gateway 12 is coupled between the Internet 102 and a PC 202.

[0024] Fig. 4 illustrates a third network 300 in which the present invention may be practiced. The gateway 12 is coupled between a first network of any known design 302 and a second network 304 of any known design.

[0025] Fig. 5 illustrates a fourth network 400 in which the present invention may be practiced. The gateway 12 is coupled between the Internet 102 and an Internet service provider 400. The Internet service provider 402 is coupled via modem 402 to one of a local area network or PC 104 and 202 respectively.

[0026] While the invention has been described in terms of its preferred embodiments, it should be understood that numerous modifications may be made thereto without departing from the spirit and scope of the present invention. It is intended that all such modifications fall within the scope of the appended claims.